

Implementasi *Honeypot* untuk Mendeteksi Serangan *Distributed Denial of Service* (DDoS)

¹⁾ Angella Puspa Dewi Prabaningtyas,²⁾ Irwan Sembiring

Fakultas Teknologi Informasi

Universitas Kristen Satya Wacana

Jl. Diponegoro 52-60, Salatiga 50711, Indonesia

Email: ¹⁾ 672011136@student.uksw.edu, ²⁾ irwan@staff.uksw.edu

Abstrack

Securing communication is a comprehensive challenge due to the increasing of threats and attacks to network security. By knowing the various of threats and attacks, we can collect broad data from the network, by using honeypot. Implemented honeypot uses low-interaction type that is honeyd and other supporting software such as apache2 and bind9. Based on the research, honeypot is successfully giving responds to Distributed Denial of Service (DDoS) attacks and giving false information such as operation system and open ports which are usually sought by attackers. Log outcome given by honeypot is processed into chart and diagrams which are shown through the network interface by using honeyd-viz software so that the administrator will find it easy to analyze the form of the attacks from the attackers and it also can be used to increase the security of the server.

Key words: *Honeypot, Honeyd, low-interaction, Honeyd-viz, DDoS, Distributed Denial of Service.*

Abstrak

Mengamankan komunikasi adalah tantangan luas karena meningkatnya ancaman dan serangan yang dilakukan pada keamanan jaringan. Pengetahuan tentang berbagai ancaman dan serangan tersebut diperoleh data yang sangat besar dari jaringan, dengan menggunakan *honeypot*. *Honeypot* yang diimplementasikan menggunakan jenis *low-interaction* yaitu *honeyd* dan *software* pendukung lainnya seperti *apache2* dan *bind9*. Berdasarkan hasil penelitian, *honeypot* berhasil berjalan dengan memberi respon terhadap serangan *Distributed Denial of Service* (DDoS) dan memberikan informasi palsu seperti sistem operasi serta *port-port* terbuka yang biasanya dicari oleh *attacker*. Hasil log yang diberikan oleh *honeypot* diolah menjadi grafik dan diagram yang ditampilkan melalui *web interface* menggunakan *software honeyd-viz* sehingga administrator mudah dalam menganalisis bentuk serangan *attacker* serta dapat digunakan untuk meningkatkan keamanan pada server.

Kata Kunci: *Honeypot, Honeyd, low-interaction, Honeyd-viz, DDoS, Distributed Denial of Service.*

¹⁾ Mahasiswa Program Studi Teknik Informatika, Fakultas Teknologi Informasi, Universitas Kristen Satya Wacana

²⁾ Staf Pengajar Fakultas Teknologi Informasi, Universitas Kristen Satya Wacana.